SIM Based Authentication as Payment Method in Public ISP Access Networks

5 ## BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a method and system for charging a user (client) for obtaining access to a packet data network.

10

Description of the Prior Art

A user (person, PC and communications device, such as a telephone) typically obtains access to a packet data network, such as an IP network (internet), by connectivity provided by a corporate access network or a public internet

15 service provider (ISP). The connectivity provided by the corporate access network or the ISP provides the user with a whole host of services which are billed to the user's account or to the company's account. These services are the

20 same services the user wishes to access during roaming. In certain circumstances, when the user roams, such as when a roaming agreement exists between the user's home network and a wireless network to which the user roams, through which connectivity is made to a packet data network, all charges

25 are handled automatically by the roaming agreement between the respective networks. As a result, billing consequent from the user's connectivity to the packet data network through the second network is handled seamlessly through the

billing arrangement which the user has with the first network.

However, in some situations which are especially prevalent with wireless networks which provide users access to packet data networks, the typical user may wish to remain anonymous with respect to the second network which provides connectivity to the packet data network or when there is no roaming agreement in existence to bill the user between the user's home network and the network to which the user roams and through which the user is connected to the packet data network. In these circumstances, alternative billing arrangements must be made.

The GSM (Global System for Mobile Communications) telephony system uses algorithms in the mobile user units and in the network servers which control authentication of the user to prevent unauthorized access to the network and to provide encryption of the transmissions between users. The GSM System is described in depth in the publication, "The GSM System for Mobile Communications" by Mouly and Pautet, Copyright 1992, which publication is incorporated herein by reference in its entirety. Authentication in a GSM network is performed by the generation of a signed response SRES by both the user mobile and the network which is a function of a unique secret identifier Ki of the user mobile and a random number RAND. The signed response SRES is calculated in a subscriber identification module (SIM) based on Ki inside SIM and RAND obtained from the network

2

authentication center (AUC). Additionally, the user mobile
and the network each perform encryption by generating a
ciphering key Kc, which is a function of the same random
number RAND and the secret identifier Ki of the user mobile.
5 The first authentication algorithm which calculates SRES is
known as the A3 algorithm and the second algorithm which
computes Kc, which is computed each time a mobile station is
authenticated, is known as the A8 algorithm. However, each
of the operations of authentication and computing of the
10 ciphering key Kc requires the user mobile to be programmed
to perform the aforementioned computations.

SUMMARY OF THE INVENTION

The present invention provides a method and system for
15 payment by a first network on behalf of a user to a second
network for connectivity of the user through the second
network to a packet data network such as an IP network. The
invention utilizes a series of communications between the
user, a security server of the network which provides
20 billing for communications by the user through the first
network, a public security server and an access server of a
second network through which connectivity between the user
and the packet data network is provided. The first series
of communications are characterized as purchase
25 communications in which the user inputs a user request to
the first network which requests that the user be authorized
for connection to the packet data network through a second

3

network for a specified quantity of communications, which
are referred hereinafter as "service units". Service units
without limitation may be in terms of a specified time of
connection of the user through the second network to the
5 packet data network or, alternatively, for a fixed monetary
value which provides a variable quantity of connection time
to the packet data network depending upon a rate structure
which varies depending upon the time of connection or other
factors. The user's home security server transmits to the
10 public security server of the second network the user
request and an authorization of payment by the first network
to the second network for the user's use of the packet data
network through the second network. Thereafter, the second
network transmits to the first network authentication
15 information granting user authentication to obtain
connection through the second network to the packet data
network. Calculation of the authentication information by
the second network is performed by a resident SIM which
performs a calculation analogous to the SIM in the GSM
20 system. The authentication information is transmitted from
the first network to the user which informs the user that
authentication to obtain connection to the packetized data
network has been obtained. The user request includes
a quantification of connectivity of the user to the packet
25 data network with the quantification comprising at least one
service unit with each service unit being encoded with a
random number. Preferably each service unit is encoded with

4

a different random number. The authentication information further comprises a shared key which may be used to create secure communications between the user and the packet data network. The authentication information is calculated by

5 a subscriber identification module SIM and includes a number n of service units with each service unit comprising a different random access number uniquely identifying each service unit, a signed response, and the shared key.

Preferably, the inputting of the user request to the

10 first network, the transmitting of the user request and authorization of payment to the second network and the transmitting of the authentication information from the second network to the first network and to the user are by secured communications. Therefore, the transmitting of the

15 shared secret key Kc is not open to the public and furthermore, it is not necessary, as with GSM communications, for the user's mobile to contain the algorithms to compute the shared secret key Kc in order for during subsequent communications between the user and the

20 packet data network for secured communications to be established between a user and the packet data network.

The consumption of the authorized service units occurs after the user has been informed that access to the packet data network has been granted and is initiated by the user

25 transmitting to the second network, such as, but not limited to, during roaming, at least one request for consumption of at least one service unit comprising a random number and a

signed response. The second network compares the random

number and the signed response of each request for

consumption of at least one service unit received from the

user with stored random numbers and signed responses to

5 determine if a match exists. If a match exists, the second

network permits data packets to pass through the second

network between the user and the packet data network. The

second network debits from a stored value of n service units

which have been granted to a user a number of consumed

10 service units which are identified in each request for

consumption of at least one service unit until the number of

consumed service units equals the number of n granted

service units. In a preferred application, each unused

service unit is stored in the second network in a first list

15 and each used service unit is stored in the second network

in a second list. Preferably, the first and second lists

are hash tables which avoid potential collisions of service

units.

A system in accordance with the invention includes a

20 user; a first network which is connectable to the user;

a second network which is connectable to the first network

and to the user; and a packet data network which is

connectable to the second network; and wherein the first

network, in response to a user request to the first network

25 that the user be authorized for connection to the packet

data network through the second network, transmits to the

second network the user request and an authorization of

6

payment by the first network for the use by the user of the packet data network, the second network transmits to the first network authentication information granting the user authentication to obtain connection through the second

5 network to the packet data network, and the first network transmits to the user authentication information which informs the user that authentication to obtain connection to the packet data network has been obtained.

10 BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates the method of purchasing service units in accordance with the present invention by a user with a first network to provide connection to a packet data network through a second network.

15 Fig. 2 illustrates the consumption of purchased service units obtained by the method illustrated in Fig. 1 by a user during connection to a packet data network through the second network.

Like reference numerals and terminology identify like

20 parts throughout the drawings.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 1 illustrates a diagram of the purchase of service units billed by a first network 10 to a user 12 to provide

25 connection of the user (e.g. computer and modem) to a packet data network 14 through a second network 16. The billing of the purchase is by the first network 10 to the user 12. The

7

purchase is n service units of connectivity by the user

through the second network 16 to the packet data network 14

which are consumed by connection of the user through the

second network 16 to the packet data network. It should be

5 understood that the second network 16 is not limited to a

single entity and may be comprised of a plurality of

geographically separated access networks which may be

implemented with different technologies. The second network

may be any type of access network through which the user 12

10 obtains access to the packet data network 14. As

illustrated, the connectivity of the user 12 to the first

network 10 is via a wireless link 18 which may be provided

by any type of wireless service, such as, but not limited to

cellular, PCS, 802.11, wireless LAN, etc., but it should be

15 understood that any type of connectivity to the first

network 10 is within the scope of the invention, including

wireline. The illustrated connectivity of the user 12 to

the packet data network 14 via communication line 20 is

conventional and is not part of the present invention. The

20 purchase of the n service units, wherein n is any integer,

is later used for authentication and billing the user 12

when the user accesses the packet data network 14 through

the second network 16 as illustrated in Fig. 2 as explained

below.

25   The initial purchase sequence involves four steps for

purchasing the n service units as illustrated in Fig. 1.

8

The first step "1" involves the inputting by the user 12

from the user's processor a user request requesting purchase

of the n service units which is transmitted to the home

security server 24 of the first network 10. The purchase of

5 n service units provides access and specifies a quantity or

value of communications to the packet data network 14

through the second network 16. The purchase of n service

units is transmitted to a home security server 24 in the

first network 10 to provide the user with authority for

10 connection to the packet data network 14 through the second

network 16 which, in a preferred application, provides

connectivity to the packet data network when the user 12 is

roaming.

The second step is a transmission "2", between the home

15 security server 24 and the public security server 26 of the

second network 16 which quantifies the n service units by

assigning a unique identifying random number RAND to each

service unit. Alternatively, each unique RAND could be

generated by the user 12 and forwarded to the home security

20 server 24 as part of the n service units.

The communications between the home security server 24

and the public security server 26 are via a secure link 28.

The access server 30 of the second network 16 is connected

to the public security server 26 by secure communication

25 link 32. The access server 30 in combination with the

public security server 26 controls passage of packets

between the second network 16 and the packet data network 14

over the unsecured communication link 22 as described below
in conjunction with Fig. 2. Preferably, the user request
over link 18 to the home security server 24 and the
transmission on n random numbers identifying the n service
5 units to be purchased from the second network 16 between the
home security server and the public security server 26 are
via a secure link. The second transmission "2" between the
home security server 24 and the public security server 26 in
addition to the quantification of n service units, which are
10 each preferably individually encoded as a unique random
number RAND, includes an authorization of payment,
preferably in terms of electronic payment (E cash).
However, the payment may be any mechanism for clearing
payment from the first network 10 to the second network 16
15 to secure the user's connectivity to the packet data
network 14.

The public security server 26 calculates the n service
units and stores them in a first list which may be
preferably a hash table storing the number of unused service
20 units. Furthermore a second list, which may preferably be
a hash table, accounts for consumed service units from the
n authorized service units. Alternatively, the second list
may be eliminated by deleting the consumed service units
from the first list as they are consumed. The hash tables,
25 which rely upon well-known hashing functions which are well
known and are not described in detail in view of their known
status, provide a unique address for locating all of the

10

n authorized service units during their history from authorization to consumption. During the consumption phase, as described below in Fig. 2, the unused and used service units are accounted for in order to insure that only

5 the purchased amount of connectivity (time or monetary value) of the user 12 to the packet data network 14 occurs.

The third step in the purchase phase is a transmission "3" from the public security server 26 of the second network 16 to the first network of authentication

10 information in the form of n information triplets each corresponding to information necessary to encode an individual service unit. The authentication information preferably includes for each service unit the individual random numbers RAND, a signed response RES, which is

15 calculated in a manner identical to the signed response calculated by GSM authentication using the prior art A3 algorithm, and the cipher key Kc which may be used to provide secure communications between the user 12 and the packet data network 14 through the second network 16. The

20 cipher key Kc is also a shared key between the access server 30 and the user 12 in the consuming phase of Fig. 2.

The fourth step in the purchase phase is a transmission "4" during which the home security server 24 receives the authentication information comprising the

25 n triplets of RAND, SRES, Kc and forwards the n triplets to the user 12 which informs the user that the purchase of service units for consumption in the data network 14 has

11

been completed. The fourth step completes the purchase sequence which enables the user 12 to secure either fixed time units of connectivity to the packet data network 14 through the second network 16 or a variable number of

5 service units representing connectivity which is variable as a function of time (prime time and off time) or other criteria.

It is important to note that upon receipt of the authentication information by the user 12, the user and the

10 public security server 26 have in storage the shared secret cipher key Kc necessary for establishing secured transmissions between the user and the packet data network 14 through the second network 16 during the consumption of the n service units. The generation of the

15 signed response SRES and the shared secret cipher key Kc by the public security server 26 and transmitting the same back to the home security server 24 via secure communication link 28 and from the home security server to the user 12 eliminates the requirement that the purchase of service

20 units requires the user's processor to have the A3 and A8 algorithms present (which are utilized in GSM authentication) to purchase and consume service units in view of the public security server 26 being the source of the initial calculation of the shared secret cipher key Kc

25 necessary for producing the secured communications or/and the user authentication.

The second consumption phase of the method of the present invention involves three steps which are illustrated in Fig. 2. As illustrated, the user 12 has roamed (moved from connection to the first network 10) and accesses the

5 second network 16 via link 18' which preferably is a wireless link but it should be understood that the invention is not limited thereto. The access server 30 controls the access of the users to the second network 16 and optionally the traffic of data packets between the user 12 and the

10 packet data network 14 during the consumption of the n service units. However, the access server may only perform authentication when the user 12 is newly connected to the second network 16 and thereafter, the access server may not be involved at all with the data exchange between the user

15 and the packet data network 14 during the user's connection to the second network.

The first step involves the user 12, after the user has been informed that authorization for connection to the packetized data network 14 has been obtained, transmitting a

20 first communication "1" to the access server 30 of the second network 16 via link 18' containing at least one access request. Each access request contains an individual random access number RAND and a signed response SRES which comprise identification of each service unit.

25 The second step involves a transmission "2" which is an access request that is relayed from the access server 30 to the public security server 26. The public security

13

server 26 compares each random number RAND and the signed

response SRES of each request for consumption of at least

one service unit received from the user 12 with the stored

random numbers RAND and signed responses SRES stored in the

5 public security server to determine if a match exists. If

the public security server 26 detects that a match exists,

the access server 30 of the second network 16 permits the

data packets of communications between the user 12 and the

packet data network 14 to pass through the second network

10 between the user 12 and the packet data network 14.

The public security server 26 of the second network 16

debits from the stored value n of service units in the first

list or hash table, which have been granted to the user 12

as a consequence of payment terms being reached between the

15 first network 10and the second network 16, a number of

consumed service units which are identified in each request

for consumption of at least one service unit until the

number of consumed service units equals the number of

n granted service units. The second optional list or hash

20 table stores those service units which have been returned to

the public security server 26 and verified as having been

consumed. Therefore, a running total is maintained in the

public security server 26 at all times of those service

units which have been granted, those service units which are

25 consumed and those service units which are not consumed or,

alternatively, if the second list is not used, only the

first list of unconsumed service units is kept with the

consumed service units being deleted therefrom. Upon each

service unit being matched by the public security server 26,

the cipher key Kc is calculated from the list based on each

service unit's random number RAND and the signed response

5 SRES.

The third step is a transmission "3" which is an access

grant permitting the user 12 and the packet data network 14

to communicate through the second network 16. The cipher

key Kc is used to encrypt the access granted to the user 12

10 to the packet data network 14 through the unsecured

communication path 22 between the second network 16 and the

packet data network. If, on the other hand, a match is not

obtained between a received service unit at the public

security server 26 and the stored service units, then the

15 access server 30 denies connectivity between the user 12 and

the packet data network 14 via the unsecured communication

path 22.

It should be understood that the present invention is

not limited to the network architecture discussed above and

20 may be practiced in diverse network configurations.

Furthermore, the design of the networks in which the present

invention is practiced is well known and in itself is not

part of the present invention. Additionally, the

methodology used for encoding of the transmissions between

25 the user 12, the first network 10 and the second network 16

during the purchase and consumption methods of Figs. 1 and 2

may be accomplished in diverse ways which is not part of the present invention.

While the invention has been described in terms of its preferred embodiments, it should be understood that numerous 5 modifications may be made thereto without departing from the spirit and scope of the invention as defined in the appended claims. It is intended that all such modifications fall within the scope of the appended claims.